REMARKS

Claims 1-7, 9-12, and 16-18 are pending in this application. Claims 1-7, 9-12, and 16-18 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,860,128 (Nakagawa). Claims 1-7, 9-12, and 16-18 have been further rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,032,257 (Olarig). Claims 1-7, 9-12, and 16-18 have been further rejected under section 102(b) as being anticipated by U.S. Patent No. 5,778,421 (Nagano). Claim 2 has been cancelled. Claims 1, 3, 4 and 11 have been amended. No new matter has been added.

Applicant notes that in page two of the Examiner's 35 U.S.C. § 102(b) rejection of the claims by Nakagawa the Examiner makes reference to Nagano. Applicant assumes that this is a typo and that that the Examiner meant to write Nakagawa because anticipation under 35 U.S.C. § 102(b) requires all elements of the claims to be found in a single reference.

Independent claims 1 and 11 as amended includes features not found in the prior art of record. Specifically, independent claim 1 as amended recites:

> A method of recording data comprising the acts of:
>> receiving protected content at a data processing
> device;
>> **determining that a portable memory**
> **recording device is trustworthy based on a proprietary**
> **physical hardware interface between said data processing**
> **device and said portable memory recording device, wherein**
> **determining that said portable memory recording device is**
> **trustworthy includes determining that said portable**
> **memory recording device will not record said protected**
> **content onto portable memories falling outside of a class;**
> **and**
>> using said portable memory recording device to
> record said protected content onto a portable memory.

Nakagawa purports to teach a system for authenticating recordable media (Nakagawa, Abstract). A recessed embossment is made in the recordable medium (Id.) The media player has a raised version of the same embossment (Id). When the recordable medium is inserted into the media player, the recessed embossment on the recordable medium if fitted into the raised version in the player (Id.). If the embossments do not fit together then the recordable medium is rejected as unauthentic, else, the recordable medium is successfully authenticated (Id.).

Olarig purports to teach a method of theft protection for computer related hardware (Olarig, Abstract). A digital handshake between a system and the hardware is performed, and if unsuccessful, the hardware is either crippled or disabled (Id.).

Nagano purports to teach a an information processing system for a disk-like storage medium such as flexible magnetic disks or a DVD-RAM (Nagano, Abstract). The disk-like storage devices comprise disk image data, as well as several other data sections (Id.). The disk sections are related together such that the legitimacy of the image data may be verified by confirming the relationships between the data sections (Id.).

Neither Nakagawa nor Olarig nor Nagano, alone or combination, teach **determining that a portable memory recording device is trustworthy based on a proprietary physical hardware interface between said data processing device and said portable memory recording device, wherein determining that said portable memory recording device is trustworthy includes determining that said portable memory recording device will not record said protected content onto portable memories falling outside of a class** as set forth in amended claim 1.

As to Nakagawa, the Examiner states that Nakagawa teaches **determining that said portable memory recording device will not record said protected content onto portable memories falling outside of a class** (Office Action, page 2). To the contrary, Nakagawa teaches a method for authenticating portable media, there is no teaching in Nakagawa of determining if a device is trustworthy based upon a proprietary interface between the processing device and a portable memory recording device. As shown in Nakagawa, a floppy disk (portable media) is given an embossed symbol that couples with a matching raised symbol in the media player. If the symbols do not couple, then the media player will not play the floppy.

This is not the same as **determining that said portable memory recording device will not record said protected content onto portable memories falling outside of a class**. In the system disclosed by Nakagawa, the portable memory recording device is the floppy disk drive that receives the floppy disk and checks for the embossed portion. The purpose of checking the embossed portion by the floppy disk device to determine if the floppy disk is authentic, and has nothing to do with determining if the floppy disk drive (the portable media device) will not record the contents of the floppy disk (the protected content) to a portable

memories falling outside the class. Nakagawa teaches authenticating media by the media recording device, wherein claim 1 is directed to checking the trustworthiness of the media player itself. The system of Nakagawa is entirely incapable of determining the trustworthiness of the media player itself, only the media. In Nakagawa, the floppy disk is given a recessed embossment, thus would be capable of being read by any standard floppy disk player because the recessed embossment would necessarily not interfere with the operation of the floppy disk drive. It is only the modified floppy disk drives with the raised embossment that are incapable of playing disks without the corresponding recessed embossment. Thus the system of Nakagawa is entirely incapable of determining the trustworthiness of a media player, only the media itself. Because Nakagawa fails to teach or suggest features of claim 1, it is respectfully requested that the Examiner withdraw the rejection and allow claim 1.

As to Olarig, Olarig is directed to the problem of computer component theft (Oliarg, col. 1, ll. 24-30). Specifically, Olarig recognizes that the proliferation of plug and play and hot swapping component architectures (i.e., non-proprietary interfaces) have made component theft easy for thieves (Id., col. 1, ll. 31-34). Because plug and play devices use a standard non-proprietary interface, e.g., PCI, ISA, USB, etc., a thief is guaranteed that a device stolen from any given computer will likely be operational on other computers, thus ensuring a market for the stolen device.

Olarig solves the problem of theft by incorporating an authentication code into the computer devices (Olarig, col. 3, ll. 17-30). When the computer system powers up, it performs a handshake operation with each of the installed computer devices where a stored authentication code on the system is compared against the authentication codes of the devices (Id.). If the devices can't be authenticated, i.e., the codes don't match, then the system disables them (Id.). Thus, a thief would have no reason to steal the installed devices because they would be presumably inoperable on other computer systems, even though the devices use a standard plug and play type interface.

Applicant has amended claim 1 to clarify that the **proprietary hardware interface is physical, thus includes no electronic type authentication codes**. Thus, the system of Olarig which relies on proprietary electronic authentication codes, and not proprietary physical hardware cannot teach or suggest such feature as shown in claim 1.

Similarly, Nagano teaches the use of non-proprietary interfaces (e.g., DVD-RAMS), and relies on a mathematical relationship between a first data stored on the medium and a second data stored on the medium. Thus, the system of Nagano cannot not teach or suggest a physical proprietary hardware interface, because it relies on the combination of standard non-proprietary media (DVD-RAMS) along with a particular software (non-physical) method for storing the data.

Because neither Nakagawa nor Olarig nor Nagano, alone or combination, teach **determining that a portable memory recording device is trustworthy based on a proprietary physical hardware interface between said data processing device and said portable memory recording device, wherein determining that said portable memory recording device is trustworthy includes determining that said portable memory recording device will not record said protected content onto portable memories falling outside of a class** as set forth in amended claim 1, it is respectfully requested that the Examiner withdraw the rejections and allow claim 1.

Claim 11 as amended contains similar (although not identical) features as claim 1, and is therefore allowable for at least the reasons given above with respect to claim 1. It is therefore respectfully requested that the Examiner withdraw the rejections and allow claim 11.

Dependent claims 3-7, 9, 10, 12, and 16-18 are all variously dependent on independent claims 1 and 11, and are therefore allowable for at least the reasons given above for the independent claims. It is therefore respectfully requested that the Examiner withdraw the rejection and allow claims 3-7, 9, 10, 12, and 16-18.

CONCLUSION

For the reasons set forth above, claims 13-7, 9-12, and 16-18 have been shown to be patentable over the applied prior art. Applicant submits that the case is in condition for allowance, and requests favorable action on the merits.

Date: December 21, 2005

_____
Michael W. Tieff
Registration No. 57,845

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439